PDR RID Report

Date Last Modified 4/25/95
Originator Chris Lynnes
Organization GSFC DAAC
E Mail Address lynnes@daac.gsfc.nasa.gov
Document CSMS PDR - Day 3

Phone No 301-286-2260

RID ID PDR	248
Review	CSMS
Originator Ref	GDAAC-MSS-23
Priority	2

Section **Page** **Figure Table** CW2-2

Category Name Design-MSS **Actionee** HAIS

Sub Category

Subject Security - Physical Measures

Description of Problem or Suggestion:

DAAC Facility Access may be inadequate to ensure Kerberos security, which through a single point of attack (the security server) can provide a network-wide breach. The DAAC Facility may be shared with other projects (as in GSFC V0) may have visitors from time to time, may support summer students or visiting scientists, etc. Current facility practices are not completely relevant as Kereberos is not deployed, and is host-by-host.

Originator's Recommendation

Find out whether current accepted practice for Kerberos/DCE security requires a security closet for the security server, and separation of the security servers from other DCE servers.

GSFC Response by: **GSFC Response Date**

HAIS Response by: Forman **HAIS Schedule** 2/28/95

HAIS R. E. C. Wheatly **HAIS Response Date** 2/28/95

This RID requests that an investigation be made to determine if, 1) a security closet if required for the security server, and 2) if separation of the security server from other DCE servers is required. These two recommendations are discussed separately below:

1. The RID recommendation suggests the use of a security closet as a form of physical security protection to the security server. Physical separation of the security server and several other ECS servers from other DAAC computing resources is strongly encouraged if current DAAC facility security practices are not upgraded. The physical protection of these collections of servers are seen primarily as GFE facility measures to comply with physical access requirements in accordance with the NASA Automated Information Security Handbook, NHB 2410.9A. NHB 2410.9A calls for physical controls to allow physical and/or logical control over authorization for and access to the systems and processing resources, and physical protection to prevent anauthorized access, theft or destruction of system resources.

A separate security closet around the security server is not required with appropriate facility-level security measures. Even if implemented, the security server closet would not provide an adequate level of physical security protection to other equally critical ECS assets. Comparable or greater security breaches can result through directed attacks on the directory server, several SDPS specific servers (i.e., select Data Management and Data Server subsystem servers), and FOS equipment. For this reason, facility access measures of several ECS resources are needed, and a single security closet around the security server alone is not sufficient to meet the ECS facility-related physical security requirements for the DAACs. The security closet is viewed by the CSMS designers as a room or building with physical access controls to physically protect several key ECS resources, negating the need for standalone security closets around individual servers. The Security Plan (CDRL 214), due next month will provide a section 3.4 on the ECS security approach to further elaborate physical security findings and requirements at the DAACs.

2. The physical combining of the directory and security servers was done to enhance system performance, lower system costs, improve overall system RMA, and improve M&O administrator efficiency. While physically integrated, the services of the CSS/MSS server configurations are logically separated, with distinct access controls and ticket grants. The PDR design assumes DAAC facility compliance with NHB2410.9A security requirements, which include physical access protection of system resources. Under this assumption, physical separation of the security server to protect against unauthorized access, theft or destruction is not required. With DAAC facility compliance, system administrator access to the security server is physically protected, and security updates and maintenance to the security server are done without compromise. In lieu of adequate facility-level physical security measures, the user access to the security server is readily constrained through a display terminal directly connected to the server and physically accessed by an administrator inside a locked room or protected cubicle. This is accomodated through the physical placement of the administrator display terminals and does not affect the CSS/MSS server configurations as provided at PDR and documented within the L4 specfication.

PDR RID Report

directly connected to the server and physically accessed by an administrator inside a locked room or protected cubicle. This is accomodated through the physical placement of the administrator display terminals and does not affect the CSS/MSS server configurations as provided at PDR and documented within the L4 specfication.

Status	**Closed**	**Date Closed**	**4/25/95**	**Sponsor**	**Broder**

******** Attachment if any ********